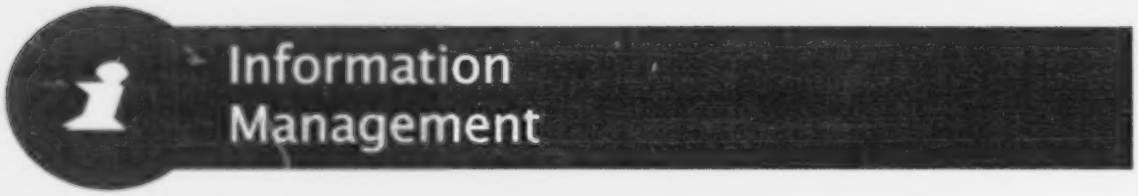


Information Security Classification Guide

Discussion Draft
April 2004

Alberta
GOVERNMENT OF ALBERTA

Produced by

Information Management Branch
Government and Program Support Services Division
Alberta Government Services
3rd Floor, Commerce Place
10155 – 102 Street
Edmonton, Alberta, Canada
T5J 4L4

Office Phone: (780) 422-2657
Fax: (780) 427-1120

Web sites:
www.im.gov.ab.ca
www.gov.ab.ca/foip
www.pipa.gov.ab.ca

©Government of Alberta

ISBN 0-7785-3107-4

Contents

1. Introduction 1
Why security classification is important 1
The need for a common approach 2
Related legislation, policies and standards 2

2. Classifying Information Assets 6
Approach 6
Security classification guideline 7

3. Information Security Classification in Practice 10
Labeling information 10
Storing information 11
Transmitting information 12
Protecting the integrity of information 13
Allowing appropriate access and disclosure 14
Establishing accountability 14

4. Implementing Information Security Classification 18

Appendix 1: Comparison with Other Jurisdictions 22

1. Introduction

The Government of Alberta is committed to managing its information assets to support service delivery to Albertans, efficient and effective operations and to protect the value of its investments. The Information Management Framework[1] outlines principles and directives for managing all government information assets. Information security is an important part of this asset management framework. This guide includes a standard approach to security classification and guidance for ministries on its use.

Why security classification is important

There are several reasons why ministries should be concerned about information security classification. These include:

- **Protection of personal information**. The *Freedom of Information and Protection of Privacy Act* governs the collection, use and disclosure of personal information. The Act also governs the management of personal information – its protection, retention, and accuracy. Security standards support the effective application of the Act in the conduct of day-to-day business.
- **Protecting confidential information from unauthorized access.**. In the normal business of government, certain information must remain confidential (for example, the annual Provincial Budget). In other instances, information may be need to be protected to comply with relevant legislation such as the *Health Information Act*. Applying proper security classification and practices can safeguard against unauthorized access to confidential government information.
- **Protecting intellectual property**. The Government of Alberta has significant investments in intellectual property. The Information Management Framework requires that these investments be protected to benefit Albertans. Appropriate security practices are needed to ensure an adequate level of protection.
- **Supporting routine disclosure and active dissemination**. Under the Information Management Framework, ministries are required to develop

[1] The framework, "Managing Information Assets in the Government of Alberta," was adopted by Deputy Ministers' Committee in April, 2003. It is available at www.im.gov.ab.ca.

plans for the routine disclosure and active dissemination of information to Albertans. Security classification of information assets is a critical component in identifying and facilitating the disclosure and dissemination of information. It can also help identify information that needs to be protected but might be inter-filed with or combined with unrestricted information.

The need for a common approach

More and more work of the government is carried out in partnership with other service providers. Moreover, secure information sharing and access is needed in an electronic service delivery (ESD) and electronic business (E-business) environment.

When information is shared with individuals outside your organization who are not aware of the value or sensitivity of an information asset, it becomes essential that the sensitivity level be established so that information requirements can be quickly understood, communicated and acted upon.

Intergovernmental cooperation and integrated service delivery will require a consistent approach to security classification.

These guidelines have been developed to be consistent with other jurisdictions in Canada (see Appendix 1).

Related legislation, policies and standards

Information security classification should be viewed in the context of related legislation, policies and other standards in the Government of Alberta.

Freedom of Information and Protection of Privacy Act (FOIP)

FOIP legislation governs the public's right to access government information as well as the collection, use and disclosure of personal information.

The legislation also governs the management of personal information – its protection, retention and accuracy.

Standards and practices related to the legislation can be found in the Freedom of Information and Protection of Privacy Guidelines and Practices Manual www.gov.ab.ca/foip/guidelines_practices/index.cfm

NOTE: A decision to deny access to a record or any part of it related to an access request under the *Freedom of Information and Protection of Privacy Act* must be based **solely** on the exemption provisions of FOIP as they apply at the time the request is made and must **not** be based on a security classification.

Health Information Act

The Health Information Act governs the handling, use and sharing of information related to the health of individuals in the province.

Standards and practices related to the legislation can be found in the Health Information Act Guidelines and Practices Manual at: http://www.health.gov.ab.ca/resources/publications/pdf/HIAguidelines2.pdf.

Records Management Regulation

Under the Records Management Regulation, all ministries are required to develop records retention and disposition schedules related to the length of time records must be kept (retention) and how records are to be disposed of (either through destruction or transfer to the Provincial Archives of Alberta). Under this regulation, the Minister responsible for the regulation may establish policies, standards and procedures for the security of records under the control of the Government of Alberta.

Information Management Framework

Deputy Ministers adopted the Information Management Framework (IMF) www.im.gov.ab.ca/imf/pdf/IMFrameworkSummary.pdf to bring greater discipline and consistent practices in the management of all information assets. The IMF outlines six broad principles related to the management of information assets. These principles are to be achieved through 18 directives for ministries. Policies, standards and practices (such as this information security classification standard) support the achievement of the IMF directives.

Information and Communications Technology (ICT) Security Framework

In today's world, threats to the security of information and information technology assets are constant. The ICT Security Framework establishes a comprehensive plan to enable the Government of Alberta to be vigilant and effective in protecting these assets from disruption, unauthorized access or corruption of the electronic information. Supporting this framework are

security policies, security architecture, technical standards and documents of best practices. These include:

- Information Technology Security Policy
  www.sharp.gov.ab.ca/showobject.cfm?docnumber=3882
- Information Technology Baseline Security Requirements
  www.sharp.gov.ab.ca/showobject.cfm?docnumber=3078
- Government of Alberta Internet and E-Mail Use Policy
  www.sharp.gov.ab.ca/showobject.cfm?docnumber=2007
- Security Policy for Disk Wiping Surplus Computers
  www.sharp.gov.ab.ca/showobject.cfm?docnumber=2356
- Wireless LAN Access Security Policy
  www.sharp.gov.ab.ca/showobject.cfm?docnumber=3867
- Threat and Risk Assessment Guidelines
  www.sharp.gov.ab.ca/showobject.cfm?docnumber=3047
- GAEA Security Architecture
  www.sharp.gov.ab.ca/showobject.cfm?docnumber=4124

Information and Communications Technology (ICT) Privacy Framework

The ICT Privacy Framework establishes a strategy for the protection of privacy in GoA information and communications technology operations. It has two key features:

- a set of ICT Privacy Principles provide general direction for ICT privacy protection in the Government of Alberta; and
- the GAEA Privacy Architecture lays out specific privacy design standards and guidelines for applications of information and communications technology in the Government of Alberta.

The ICT privacy principles and an overview of the privacy architecture are available at www.sharp.gov.ab.ca/ppa.

Policy for the Protection of Personal Information in Information Technology Outsource Contracts

As ministries rely on outside providers to support the delivery of information technology to staff and the public, this policy [www.sharp.gov.ab.ca/showobject.cfm?docnumber=3293] outlines the responsibilities of government to ensure that service providers protect personal information.

Policy for the Transmission of Personal Information via Electronic Mail and Facsimile

Public communication networks such as the Internet and other telecommunications networks are not totally secure environments. Ministries must take steps to protect personal information when it is transmitted over these public networks. The policy can be accessed at www.sharp.gov.ab.ca/showobject.cfm?docnumber=3546.

104-057937

2.
Classifying Information Assets

Approach

Ministries will determine the extent to which security classification needs to be applied to information assets.

The security classification of information assets should meet both business and operational needs. It should be based on a threat and risk assessment and business impact analysis.

Criteria

Four criteria are the basis for deciding the security and access requirements for information assets. These criteria are:

- **Integrity**: information is current, complete and only authorized and accurate changes are made to information;
- **Availability**: authorized users have access to and can use the information when required;
- **Confidentiality**: information is only accessed by authorized individuals, entities or processes; and
- **Value**: intellectual property is protected, as needed.

Threat and risk assessment

These criteria can be applied in a threat and risk assessment. The purpose of the assessment is to identify what the probability or likelihood of threat is and what the impact would be if there was a loss to the integrity, availability, confidentiality or the value of information assets. Threat and risk assessments as well as Privacy Impact Assessments (PIAs) are undertaken to properly identify risks.

The Office of the Corporate Chief Information Officer has developed Threat and Risk Assessment Guidelines for information assets. This guide to conducting threat and risk assessments can be found at www.sharp.gov.ab.ca/showobject.cfm?docnumber=3047.

The OCTAVE risk management methodology can also prove useful during risk assessments (www.cert.org/octave)

The Office of the Information and Privacy Commissioner provides guidance in the preparation of privacy impact assessments at www.oipc.ab.ca/pia.

Security classification guideline

The security classification guideline for information assets in the Government of Alberta consists of four categories. These categories, with a description, and examples of the types of records that might be found in that category are outlined in Table 1 on the following page.

This guideline has been developed to be consistent with approaches taken in other jurisdictions. Appendix 1 contains a comparison of this classification guideline with the draft security classification standard being developed by the Council of Public Sector CIOs and the information classification standard adopted by the Government of Ontario and the Office of Management and Budget (OMB) in the United States.

Table 1
Information Security Classification Guidelines

Classification	Description	Examples of Information Assets	Examples of Risk Impacts
Unrestricted	Information that is created in the normal course of business that is unlikely to cause harm. Unrestricted information is available to the public, employees and contractors, sub-contractors and agents working for the government. Unrestricted information includes information that ministries must make public under legislation or regulation.	▪ Speeches, ▪ Procedure manuals ▪ Ordinary staff meeting agendas and minutes ▪ Communications to claims clerks ▪ Research and background papers (with no copyright restrictions)	▪ Little or no impact ▪ Minimal inconvenience if not available
Protected	Information of interest to the GoA that could impact service levels or performance, or low levels of financial loss to individuals or enterprises. Protected information may include personal information, financial information or details concerning the effective operation of the GoA, ministries and departments. Protected information is available to those possessing a need to know for business-related purposes.	▪ Policy interpretation ▪ Draft request for proposals ▪ Business information ▪ Applications ▪ Planning documents ▪ Documents containing personal information ▪ Information covered by copyright	▪ Unfair competitive advantage ▪ Low levels of financial loss ▪ Disruption to business if not available.
Confidential	Information that could cause loss of privacy, competitive advantage, loss of confidence in government programs, damage to partnerships, relationships and reputation. Confidential information may include personal information, financial information or details concerning the effective operation of the GoA, ministries and departments. Access to Confidential information is specific to a function, group or role.	▪ Personal case files such as benefits, program files or personnel files ▪ Industrial trade secrets ▪ Registration information ▪ Personnel files ▪ Grade 12 Provincial Examinations ▪ Policy Advice ▪ 3rd party business information submitted in confidence	▪ Loss of reputation or competitive advantage ▪ Loss of confidence in the government program ▪ Loss of personal or individual privacy ▪ Loss of trade secrets or intellectual property ▪ Loss of opportunity (e.g., insurance, health coverage) ▪ Damage to partnerships

Table 1
Information Security Classification Guidelines

Classification	Description	Examples of Information Assets	Examples of Risk Impacts
Unrestricted	Information that is created in the normal course of business that is unlikely to cause harm. Unrestricted information is available to the public, employees and contractors, sub-contractors and agents working for the government. Unrestricted information includes information that ministries must make public under legislation or regulation.	• Speeches, • Procedure manuals • Ordinary staff meeting agendas and minutes • Communications to claims clerks • Research and background papers (with no copyright restrictions)	• Little or no impact • Minimal inconvenience if not available
Protected	Information of interest to the GoA that could impact service levels or performance, or low levels of financial loss to individuals or enterprises. Protected information may include personal information, financial information or details concerning the effective operation of the GoA, ministries and departments. Protected information is available to those possessing a need to know for business-related purposes.	• Policy interpretation • Draft request for proposals • Business information • Applications • Planning documents • Documents containing personal information • Information covered by copyright	• Unfair competitive advantage • Low levels of financial loss • Disruption to business if not available.
Confidential	Information that could cause loss of privacy, competitive advantage, loss of confidence in government programs, damage to partnerships, relationships and reputation. Confidential information may include personal information, financial information or details concerning the effective operation of the GoA, ministries and departments. Access to Confidential information is specific to a function, group or role.	• Personal case files such as benefits, program files or personnel files • Industrial trade secrets • Registration information • Personnel files • Grade 12 Provincial Examinations • Policy Advice • 3rd party business information submitted in confidence	• Loss of reputation or competitive advantage • Loss of confidence in the government program • Loss of personal or individual privacy • Loss of trade secrets or intellectual property • Loss of opportunity (e.g., insurance, health coverage) • Damage to partnerships

Restricted	Information that could cause damage to the integrity, image or effective service delivery of the GoA. Extreme damage includes loss of life, risks to public safety, substantial financial loss, social hardship, and major economic impact. Access to Restricted information is specific to a named individual and is very limited.	• Cabinet documents • Cabinet deliberations and supporting documents • Personal medical records • Provincial Budget prior to public release • Criminal Records • Criminal Investigations	• Loss of life • Extreme serious injury • Loss of public safety • Significant financial loss • Compromise of the legal system • Compromise of Cabinet deliberations • Destruction of partnerships and relationships • Significant damage • Sabotage/terrorism

NOTES:

1. If a ministry receives information from another jurisdiction that has been classified, the original classification must be retained or increased.

2. Information that has been classified at a higher level of protection can be reclassified to a lower level of protection by the information owner or originating program area only.

3.
Information Security Classification in Practice

Implementing information security classification will mean that ministries should consider practices related to:

- labeling information;
- storing information;
- transmitting information;
- disposing off unneeded information;
- protecting the integrity of information;
- allowing appropriate access and disclosure; and
- establishing accountability

This section provides **examples** of practices in these areas. The practices identified are not intended to be prescriptive. Rather, they are identified here as a guide to ministries. The actual practices that are implemented will depend on the business reason for applying security classification as well as established administrative protocols (in the case of print information assets) and information technology protocols (in the case of electronic information assets).

Labeling information

Implement standard security labels for your information assets. The actual labeling procedure will vary depending on the medium in which the information is stored.

Table 2 identifies some common labeling methods for various types of information assets.

Table 2
Sample Labelling Methods

Type	Procedure
Hard copy documents	Rubber ink-stamps for each level may be needed to mark hardcopy documents received from outside the organization
Electronic mail	Identify security classification in subject line of e-mail, if classified as confidential, or restricted.
Electronic documents	Identify security classification in document metadata. If the electronic document is to be printed or viewed in .pdf format, the security classification should appear on every page, including the cover page (this can be done by including the classification in the header/footer or by use of a watermark). Information about the ministry or department which created the document and date of creation should be included.
IT systems and applications	Identify classification in system/application metadata. Labels may be required for online screen displays and reports generated by IT systems in limited cases.
Other media	The security classification may be identified on adhesive labels applied to other media such as diskettes, CDs, DVDs, and videocassettes. A message with the classification label should be displayed when the information stored on the media is accessed.

Storing information

Depending on the security classification, information assets will need different types of storage procedures to ensure that the confidentiality, integrity, accessibility, and value of the information are protected.

Table 2
Sample Labelling Methods

Type	Procedure
Hard copy documents	Rubber ink-stamps for each level may be needed to mark hardcopy documents received from outside the organization
Electronic mail	Identify security classification in subject line of e-mail, if classified as confidential, or restricted.
Electronic documents	Identify security classification in document metadata. If the electronic document is to be printed or viewed in .pdf format, the security classification should appear on every page, including the cover page (this can be done by including the classification in the header/footer or by use of a watermark). Information about the ministry or department which created the document and date of creation should be included.
IT systems and applications	Identify classification in system/application metadata. Labels may be required for online screen displays and reports generated by IT systems in limited cases.
Other media	The security classification may be identified on adhesive labels applied to other media such as diskettes, CDs, DVDs, and videocassettes. A message with the classification label should be displayed when the information stored on the media is accessed.

Storing information

Depending on the security classification, information assets will need different types of storage procedures to ensure that the confidentiality, integrity, accessibility, and value of the information are protected.

Table 3 identifies storage procedures for printed and electronic information in the various classification categories.

Table 3
Sample Storage Procedures

Classification	Print/Hard Media	Electronic Files
Unrestricted	• No special storage requirements	• No special storage requirements • Regular back-ups to ensure availability and integrity.
Protected	• Secure location (e.g., locked office; locked file room)	• All media under physical and/or logical access control of protected zone (e.g. group authorized access etc.)
Confidential	• Secure location with restricted access • Clean desk policy	• All media under physical and/or logical access control of confidential zone(e.g. authorized access, authenticated access etc)
Restricted	• Stored in highly secure zone, with access tracking • Clean desk policy	• All media under physical and/or logical access control of restricted zone (e.g. few individuals have access, encrypted data, audit/monitoring etc.)

NOTE: Various classes of information located in one common medium/location should have the highest classification of all information located in the medium. This is important to ensure that highly classified information is not put at risk. Physical security of any media should include fire/flood/theft protection.

Transmitting information

When transmitting information that is protected, confidential or restricted, special procedures must be taken. Examples of these procedures are identified in Table 4 on the next page.

The following policies on the transmission of protected, confidential and restricted information are also applicable:

- Information Technology Baseline Security Requirements
  www.sharp.gov.ab.ca/showobject.cfm?docnumber=3078
- Government of Alberta Internet and E-Mail Use Policy
  www.sharp.gov.ab.ca/showobject.cfm?docnumber=2007
- Policy on the Transmission of Personal Information via Electronic Mail or Facsimile
  www.sharp.gov.ab.ca/showobject.cfm?docnumber=3546.

Table 4
Sample Transmission Procedures

Classification	Print/Hard Media	Electronic Files
Unrestricted	• No special procedures	• No special procedures
Protected	• Sealed envelope.	• If electronic message contains personal information, personal information must be transmitted in such a way to prevent interception, modification, or unauthorized receipt en route or at the destination (e.g., password protected file; encryption)
Confidential	• Sealed envelope, stamped confidential • Receipt confirmation required.	• Message sent in such a way to prevent interception, modification, or unauthorized receipt en route or at destination • Recipient confirmation required • Audit of access points.
Restricted	• Tamper evident packaging (e.g., double-sealed envelope with inside envelope signed to reveal evidence of tampering) • Transmitted under a continuous chain of custody with receipts covering each individual who obtains custody.	• Message sent in such a way to prevent interception, modification or unauthorized receipt en route or at destination (e.g., encryption used to send/authenticate message) • Complete audit trail of each access point.

Protecting the integrity of information

Integrity refers to the fact that information is current, complete, and only authorized changes are made to it. The integrity of information processed by and stored in information systems can be addressed by assigning the

Table 3 identifies storage procedures for printed and electronic information in the various classification categories.

Table 3
Sample Storage Procedures

Classification	Print/Hard Media	Electronic Files
Unrestricted	• No special storage requirements	• No special storage requirements • Regular back-ups to ensure availability and integrity.
Protected	• Secure location (e.g., locked office; locked file room)	• All media under physical and/or logical access control of protected zone (e.g. group authorized access etc.)
Confidential	• Secure location with restricted access • Clean desk policy	• All media under physical and/or logical access control of confidential zone(e.g. authorized access, authenticated access etc)
Restricted	• Stored in highly secure zone, with access tracking • Clean desk policy	• All media under physical and/or logical access control of restricted zone (e.g. few individuals have access, encrypted data, audit/monitoring etc.)

NOTE: Various classes of information located in one common medium/location should have the highest classification of all information located in the medium. This is important to ensure that highly classified information is not put at risk. Physical security of any media should include fire/flood/theft protection.

Transmitting information

When transmitting information that is protected, confidential or restricted, special procedures must be taken. Examples of these procedures are identified in Table 4 on the next page.

The following policies on the transmission of protected, confidential and restricted information are also applicable:

- Information Technology Baseline Security Requirements
  www.sharp.gov.ab.ca/showobject.cfm?docnumber=3078
- Government of Alberta Internet and E-Mail Use Policy
  www.sharp.gov.ab.ca/showobject.cfm?docnumber=2007
- Policy on the Transmission of Personal Information via Electronic Mail or Facsimile
  www.sharp.gov.ab.ca/showobject.cfm?docnumber=3546

Table 4
Sample Transmission Procedures

Classification	Print/Hard Media	Electronic Files
Unrestricted	• No special procedures	• No special procedures
Protected	• Sealed envelope.	• If electronic message contains personal information, personal information must be transmitted in such a way to prevent interception, modification, or unauthorized receipt en route or at the destination (e.g., password protected file; encryption)
Confidential	• Sealed envelope, stamped confidential • Receipt confirmation required.	• Message sent in such a way to prevent interception, modification, or unauthorized receipt en route or at destination • Recipient confirmation required • Audit of access points.
Restricted	• Tamper evident packaging (e.g., double-sealed envelope with inside envelope signed to reveal evidence of tampering) • Transmitted under a continuous chain of custody with receipts covering each individual who obtains custody.	• Message sent in such a way to prevent interception, modification or unauthorized receipt en route or at destination (e.g., encryption used to send/authenticate message) • Complete audit trail of each access point.

Protecting the integrity of information

Integrity refers to the fact that information is current, complete, and only authorized changes are made to it. The integrity of information processed by and stored in information systems can be addressed by assigning the

appropriate rights (e.g., read, write, modify). If the threat to the integrity of information is significant, electronic files should be saved as read only files with changes to be made only by the author (this may be handled by access rights based on user account, work group or physical access to a specific devise). In these cases, procedures must be in place for transfer of rights when the author leaves the organization.

In some cases, stronger control such as encryption may be required. In encryption is used, a process related to key escrow must be established to ensure the availability of the information.

Allowing appropriate access and disclosure

Certain types of information will require controlled access and logs to track access and disclosure activities.

Table 5 outlines the access restrictions and any special audit trail that must be maintained.

Table 5
Allowing Appropriate Access and Disclosure

Classification	Access Restrictions	Audit/Activity Files
Unrestricted	• Open to the public and all employees.	• None
Protected	• Those employees and contractors, sub-contractors and agents possessing a need to know for business-related purposes.	• Periodic audits to show protection is, in fact, occurring.
Confidential	• Limited to individuals in a specific function, group or role.	• Pre-clearance based on position or contractor, sub-contractor or agent relationship • Log of access/actions • Periodic audits of adequate protection.
Restricted	• Limited to named individuals.	• All access or actions will be logged and subject to non-repudiation processes as appropriate

Establishing accountability

A clear accountability regime for all personnel will be important to ensure the protection of government information assets. Here is a model accountability approach that ministries may want to consider:

appropriate rights (e.g., read, write, modify). If the threat to the integrity of information is significant, electronic files should be saved as read only files with changes to be made only by the author (this may be handled by access rights based on user account, work group or physical access to a specific devise). In these cases, procedures must be in place for transfer of rights when the author leaves the organization.

In some cases, stronger control such as encryption may be required. In encryption is used, a process related to key escrow must be established to ensure the availability of the information.

Allowing appropriate access and disclosure

Certain types of information will require controlled access and logs to track access and disclosure activities.

Table 5 outlines the access restrictions and any special audit trail that must be maintained.

Table 5
Allowing Appropriate Access and Disclosure

Classification	Access Restrictions	Audit/Activity Files
Unrestricted	• Open to the public and all employees.	• None
Protected	• Those employees and contractors, sub-contractors and agents possessing a need to know for business-related purposes.	• Periodic audits to show protection is, in fact, occurring.
Confidential	• Limited to individuals in a specific function, group or role.	• Pre-clearance based on position or contractor, sub-contractor or agent relationship • Log of access/actions • Periodic audits of adequate protection.
Restricted	• Limited to named individuals.	• All access or actions will be logged and subject to non-repudiation processes as appropriate

Establishing accountability

A clear accountability regime for all personnel will be important to ensure the protection of government information assets. Here is a model accountability approach that ministries may want to consider:

Deputy Minister

Deputy Ministers are responsible for the management of government records generally and have legal responsibility under the *Freedom of Information and Protection of Privacy Act* (FOIP).

Specifically, the deputy minister is responsible for:

- defining, documenting and implementing reasonable measures to prevent unauthorized access to and the inadvertent release, destruction or damage of government records; and
- safeguarding records in their custody or under their control, including records which are in the custody of third parties under alternate service delivery arrangements.

Corporate Chief Information Officer

The Corporate Chief Information Officer is responsible for establishing corporate security policy and standards for electronic information and information technology assets.

Ministry Chief Information Officer

The Ministry Chief Information Officer is responsible for:

- reviewing, understanding and applying the information security classification standard;
- recording all security breaches and violations discovered by the ministry;
- managing the response and actions taken within their ministry to breaches, violations, audits, investigations and security reviews;
- reporting these security breaches and violations along with actions taken to the Corporate Chief Security Officer and other appropriate personnel[2];

[2] The Office of the Corporate Chief Information Officer will be advised of any incidents that have the potential to affect more than one department. The *Freedom of Information and Protection of Privacy Act* Coordinator for the department will be notified if the incident involves the disclosure of personal information. The Alberta Records Management Committee will be informed of records lost. Incidents involving breaking of laws must be reported to law enforcement agencies and incidents involving physical loss or damage will be reported to Risk Management and Insurance Division, Alberta Revenue (losses in excess of $5,000.00 are covered by the Risk Management Fund)

- ensuring that implementation of the security and access standard is appropriately coordinated ministry-wide;
- guiding and assisting program managers in the assessment of their information security needs and information security classification;
- assisting staff in the identification, design and implementation of reasonable security measures;
- assisting program managers in determining if the security measures in place meet their program needs; and
- providing guidance and assistance to employees in implementing this standard.

Program Managers

Program Managers are responsible for:

- reviewing, understanding and ensuring the implementation of the information security classification standard, applicable legislation, policies and guidelines relating to the security of documents which apply to their program area;
- developing and maintaining internal procedures that support the requirements for the effective handling and security of documents;
- ensuring that all information resources under their control are identified and classified;
- ensuring that all information under their immediate control has defined appropriate retention periods and is scheduled in a manner consistent with government legislation, policies, and guidelines on records retention;
- ensuring that information under their custody or control is protected from physical damage and from unauthorized access, alteration, removal or destruction;
- ensuring that staff are aware of, trained in, and understand legislation, applicable directives and procedures relating to the security classification of government information assets; and
- reporting all actual and suspected security breaches and violations to the ministry Chief Information Officer.

Freedom of Information and Protection of Privacy (FOIP) Coordinator

The Ministry FOIP Coordinator is responsible for:

- reviewing records to determine whether any FOIP exemptions or exclusions apply when requests are received under *Freedom of Information and Protection of Privacy Act* (FOIP) for records that have a security classification **[The application of a security classification to a record does not determine whether a record is exempt from access under FOIP]**; and
- taking required action related to privacy breaches.

Senior Records Officer (SRO)

The ministry SRO is responsible for:

- providing secure locked storage facilities for protected, confidential and restricted information holdings; and
- ensuring records retention and disposition schedules are created for information holdings.

All ministry staff and staff of partners and contractors

All ministry staff and staff of partners and contractors are responsible for:

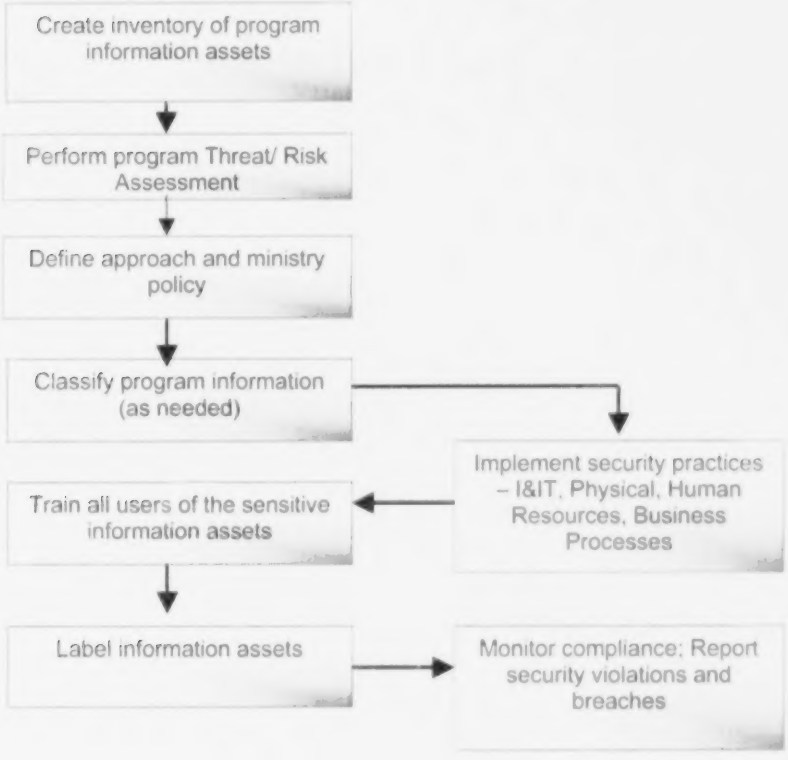
- reviewing, understanding and applying the information security classification standard to information assets they create, receive, use, transmit, or store;
- meeting their obligations under the *Freedom of Information and Protection of Privacy Act*, and the Oath of Office, to protect any information under their control or custody from unauthorized disclosure to any person or organization;
- ensuring that information under their control or custody is protected from physical damage and from unauthorized access, alteration, removal or destruction according to the security and access standard; and
- reporting all actual and suspected security and privacy breaches and violations to the Program Manager.

4.
Implementing Information Security Classification

For ministries to implement Information Security Classification, the starting point is for each ministry to develop a plan of action. This planning process should be included as part of the overall planning of information management (included in a separate forthcoming guide called Information Management Planning Guide.) Figure 1 identifies the key steps in such a plan.

The diagram below gives an overview of ministry steps in planning and implementing Information Security Classification in ministry programs.

Figure 1
Implementing Information Security Classification

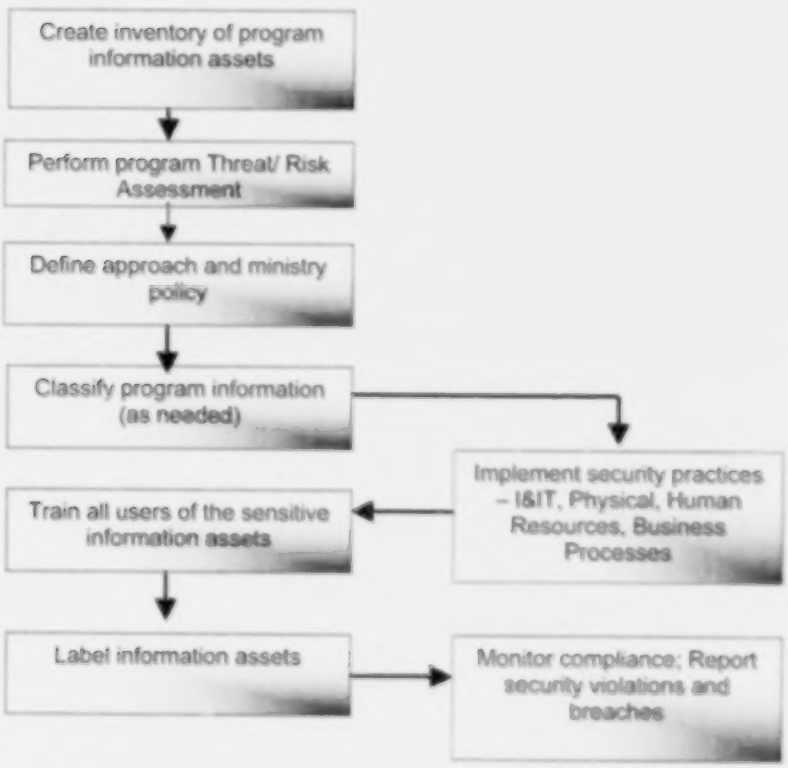

Create inventory of program information assets
Perform program Threat/ Risk Assessment
Define approach and ministry policy
Classify program information (as needed)
Implement security practices – I&IT, Physical, Human Resources, Business Processes
Train all users of the sensitive information assets
Label information assets
Monitor compliance; Report security violations and breaches

4.
Implementing Information Security Classification

For ministries to implement Information Security Classification, the starting point is for each ministry to develop a plan of action. This planning process should be included as part of the overall planning of information management (included in a separate forthcoming guide called Information Management Planning Guide.) Figure 1 identifies the key steps in such a plan.

The diagram below gives an overview of ministry steps in planning and implementing Information Security Classification in ministry programs.

Figure 1
Implementing Information Security Classification


Create inventory of program information assets
Perform program Threat/ Risk Assessment
Define approach and ministry policy
Classify program information (as needed)
Implement security practices – I&IT, Physical, Human Resources, Business Processes
Train all users of the sensitive information assets
Label information assets
Monitor compliance; Report security violations and breaches

Create an inventory of program information assets

The Records Management Regulation requires ministries to develop schedules to govern the retention and disposition of all existing recorded information under their control. The program's retention and disposition schedules are a good place to start in creating the program's inventory of documents and material assets.

Perform the threat-risk assessment

One way to assess the need for information security classification is a threat risk assessment. The purpose of the assessment is to identify what the probability or likelihood of threat is and what the impact would be if there was a loss to the integrity, availability, confidentiality or the value of information assets. Threat and risk assessments as well as Privacy Impact Assessments (PIAs) are undertaken to properly identify risks.

The Office of the Corporate Chief Information Officer has developed Threat and Risk Assessment Guidelines for information assets. This guide to conducting threat and risk assessments can be found at www.sharp.gov.ab.ca/showobject.cfm?docnumber=3047.

The OCTAVE risk management methodology can also prove useful during risk assessments (www.cert.org/octave)

The Office of the Information and Privacy Commissioner provides guidance in the preparation of privacy impact assessments at www.oipc.ab.ca/pia.

Define approach and ministry policy

Based on your assessment of your information assets, your business, and the threat risk assessment, you will need to decide which types of information you are going to apply security classification to. Once the approach has been decided, you'll need to develop policies and practices appropriate for your ministry.

Classify program information

The result of the threat risk assessment should help identify which information assets needed to be classified on a routine basis.

In preparation for labeling program documents with a security classification, you will need to determine the sensitivity of each type of document.

Even though an overall program may have been classified at a high level, individual documents within the program may have a lower security classification level than the overall program (i.e., unrestricted). There should not be any cases of a program document having a higher security classification level than the overall program. If a program document is found to have a higher security classification than the overall program then the overall program classification should be adjusted to the higher level.

Implement security practices

Information security needs to balance protection of information assets, and disclosure of information as required by legislation, regulation and good business practice. Successful implementation of information security will allow staff and service delivery agents to perform their jobs effectively while preserving the public trust.

A holistic approach means effective protection. You will need to implement security measures in information systems, human resources, physical facilities and business procedures for storage, access and use of classified information assets.

Train users

Program managers are responsible for ensuring that anyone to whom they (or their delegates or agents) provide information is fully aware and capable of meeting the required handling measures, and that unauthorized persons cannot obtain the information.

All staff who handle information that is protected, confidential or restricted need to be trained on information security classification to understand why it is important, what it means, how to label and handle the information, and how to communicate any special handling measures.

Staff who work together may be able to provide support to each other during implementation if they are trained together.

Label information assets

Implement labeling practices. Security classification labels may be required for online screen displays, reports generated by IT systems, documents created using office desktop tools, hardcopy documents received from jurisdictions, e-mail messages, and media such as diskettes, CDs and microfiche that contain sensitive information.

Monitor compliance and report violations

An effective program for information security classification will require ongoing monitoring. You will also need to establish procedures to document and report violations and breaches of security.

Appendix 1:
Comparison with Other Jurisdictions

Other jurisdictions have also developed security classification standards for information assets. The table below illustrates how Alberta's information security classification compares with standards developed in Ontario and the guidelines developed by the Council of Public Sector CIOs and the Office of Management and Budget in the United States.

Alberta	Ontario	PSCIOC	OMB (United States)
Unrestricted: Information that is created in the normal course of business that is unlikely to cause harm. Unrestricted information is available to employees and approved non-employees	**Unclassified**: Public information. Internal communications	**Unclassified**: Public information. Internal communications	**Basic**: Will not result in injury to individuals, governments or to private sector institutions or loss of under one thousand dollars.
Protected: Information of interest to the GoA that could impact service levels or performance, or inconvenience to individuals or enterprises. Protected information may include personal information, financial information or details concerning the effective operation of the GoA, ministries and departments. Protected information is available to those possessing a need to know for business-related purposes.	**Low Sensitivity**: Information that is only sensitive outside the OPS. Generally available to employees and approved non-employees	**Low Sensitivity**: Information that is only sensitive outside the government. Generally available to employees and approved non-employees.	**Low**: Could reasonable be expected to cause significant injury to individuals or enterprises that would result in financial losses, such as between one thousand and one hundred thousand dollars, a limited impact in service level or performance, embarrassment and inconvenience.

Appendix 1:
Comparison with Other Jurisdictions

Other jurisdictions have also developed security classification standards for information assets. The table below illustrates how Alberta's information security classification compares with standards developed in Ontario and the guidelines developed by the Council of Public Sector CIOs and the Office of Management and Budget in the United States.

Alberta	Ontario	PSCIOC	OMB (United States)
Unrestricted: Information that is created in the normal course of business that is unlikely to cause harm. Unrestricted information is available to employees and approved non-employees	**Unclassified:** Public information. Internal communications	**Unclassified:** Public information. Internal communications	**Basic:** Will not result in injury to individuals, governments or to private sector institutions or loss of under one thousand dollars.
Protected: Information of interest to the GoA that could impact service levels or performance, or inconvenience to individuals or enterprises. Protected information may include personal information, financial information or details concerning the effective operation of the GoA, ministries and departments. Protected information is available to those possessing a need to know for business-related purposes.	**Low Sensitivity:** Information that is only sensitive outside the OPS. Generally available to employees and approved non-employees	**Low Sensitivity:** Information that is only sensitive outside the government. Generally available to employees and approved non-employees.	**Low:** Could reasonable be expected to cause significant injury to individuals or enterprises that would result in financial losses, such as between one thousand and one hundred thousand dollars, a limited impact in service level or performance, embarrassment and inconvenience.

Confidential: Information that could cause loss of privacy, competitive advantage, loss of confidence in government programs, damage to partnerships, relationships and reputation. Confidential information may include personal information, financial information or details concerning the effective operation of the GoA, ministries and departments. Access to Confidential information is specific to a function, group or role.	**Medium Sensitivity**: Information that is sensitive within the OPS and is intended for use only by specific groups of employees.	**Medium Sensitivity**: Information that is sensitive within the government and is intended for use only by specific groups of employees.	**Medium**: Could reasonably be expected to cause serious personal or enterprise injury, loss of competitive advantage, loss of confidence in the government program, financial loss (such as between one hundred thousand and ten million dollars), legal action and damage to partnerships, relationships and reputation.
Restricted: Information that could cause damage to the integrity, image or effective service delivery of the GoA. Significant damage includes loss of life, risks to public safety, substantial financial loss, social hardship, and major economic and major political impact. Access to Restricted information is specific to an individual and very limited.	**High Sensitivity**: Information that is extremely sensitive, of highest value to the Ontario government and intended for use by named individuals (positions) only. Documents that can create an identity.	**High Sensitivity**: Information that is extremely sensitive, of highest value to the government and intended for use by named individuals (positions) only. Documents that can create an identity.	**High**: Could reasonable be expected to cause extremely serious personal or enterprise injury, significant financial loss (such as over ten million dollars), loss of life or public safety, social hardship and major political or economic impact.